UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/513,065	02/24/2000	Chi-Pei Michael Hsing	ST9-99-167	5699

7590 01/26/2005

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3213

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/513,065	HSING ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-19,21-31 and 33-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-19,21-31 and 33-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7, 9-19, 21-31, 33-43 have been examined. Applicant amended claims 25 and 37 in the amendment filed on November 12, 2004. The applicant in a previous amendment canceled claims 8, 20 and 32.

Response to Amendment

2. The 112, 2nd paragraph rejection to claim 29 is withdrawn as the amendment to parent claim 25 overcomes the rejection.

Response to Argument

3. The following is a response to Applicant's argument on pages 12-25 filed on November 12, 2004.

4. Regarding applicant's argument that the Bryant prior art is merely a dialogue suggesting theoretical design for an authentication system, and therefore is not an enabling publication (see Remarks, pg. 16, 2nd full paragraph), examiner disagrees. The publication of Bryant is a teaching of an actual authentication system that was designed and implemented at MIT's Project Athena. See Bryant, pg. 1, Abstract, 2nd paragraph.

5. Applicant's arguments that the Schneier references and Sokal references do not cover the missing limitations of Stallings and Bryant have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Stallings and Bryant.

6. Hence, Applicant's arguments with respect to claims 1-7, 9-11, 13-19, 21-23, 25-31, 33-35 and 37-43 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-7, 9-11, 13-19, 21-23, 25-31, 33-35, 42 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings) in view of Bryant "Designing an Authentication System: a Dialogue in Four Scenes" (hereinafter Bryant).

9. As per claims 1, 5, 6 and 9, Stallings discloses a simple authentication dialogue that uses a central authentication server to log a client onto a network of distributed

services. See Stallings, page 326, 'A Simple Authentication Dialogue'. This simple authentication dialogue uses a centralized server to securely identify users by obtaining information from the user; generate a ticket with the obtained user information; and then send a ticket back to the user, which comprises of an encrypted message containing the identification of the client, the network address of the client, and the identifier of the service. This generated ticket, in addition to an identifier of the client, is sent to the service, whereupon, the service decrypts the ticket and compares the identification with the parsed identification. Since only the authentication server and the service share the private encrypted key, only the authentication server could have encrypted the ticket when issued to the client. Hence, if the parsed id matches the id sent by the client, then the request is accepted. See Stallings, page 326, steps 1, 2, and 3.

10. Stallings does not explicitly disclose the ticket contains both a username and a computer identifier to authenticate a parsed username and parsed computer identifier. Bryant teaches the step of including a workstation address in the ticket issued by the Kerberos authentication method to prevent an unscrupulous workstation from intercepting an issued ticket to a valid workstation and using the ticket to access the service under the guise of the valid workstation. See Bryant, page 5, especially 8th paragraph "Athena". It would be obvious to one of ordinary skill in the art at the time the invention was made, for the identity of a user during a session to comprise a username and a computer identification as taught by Bryant in the simple authentication dialogue as taught by Stallings. Motivation to combine enables the invention to prevent identity duplicity by ascertaining a user by a unique name and a computer identifier as taught by

Bryant. Ibid. As such, the invention covered by Stallings comprises the following steps of:

a. generating an authentication key based on a user name and a computer identifier (see Stallings, page, 326, 3rd paragraph, sentence beginning with "To do so ..."; wherein the user name is the user id and the computer identifier is the workstation address);

b. receiving an authentication key, a user name, and a computer identifier (see Stallings, page 326, 3rd paragraph, step 3 as modified by Bryant, page 5, especially 8th paragraph "Athena:"; wherein the authentication key is effectively the Ticket);

c. parsing the authentication key to obtain a parsed user name and computer identifier (see Stallings page 326, 4th paragraph; 2nd sentence; definition of "Ticket");

d. validating the received user name and computer identifier using the parsed user name and computer identifier (see Stallings, page 326 2nd sentence as modified by Bryant, page 5, especially 8th paragraph "Athena:").

11. Finally, Stallings does not expressly disclose the authentication key including a server user identifier. However, Stallings teaches the aforementioned steps incorporated within the Kerberos system, wherein the user submits to a server an authentication key for access to the resources of the server (see Stallings, pg. 333, fig. 11.1, steps 5 and 6). Since, the authentication key merely authenticates the request and does not establish an identity by which the user can be identified by the server, the

inclusion of a server user identifier is an obvious enhancement. For example, Windows NT, UNIX, Linux servers all require a server user identifier to be associated with a process; any request to access these servers requires the request to be established by a known user. Furthermore, server user identifiers are also conventionally linked with a corresponding password to ensure only users who know the password to a server user identifier can be associated with the server user identifier. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication key to include a server user identifier and corresponding password. Motivation to combine facilitates identification for service to be incorporated in the authentication step, which is more efficient than separating the steps as known to one of ordinary skill in the art.

12. Hence, the invention covered above defines the following limitations: the generation of an authentication key comprising a client user name, a client computer identifier, the server user identifier, and a server password (see Stallings and Bryant, ibid); the server user identifier and corresponding password is obtained by parsing the authentication key (see Stallings, pg. 326, decryption of ticket); and the server user identifier and corresponding password enables the client to log into the server (see Stallings, page 326, step 3). The aforementioned cover claims 1, 5, 6 and 9.

13. As per claim 2, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the validating step comprises determining

whether the received user name and computer identifier match the parsed user name and computer identifier (see Stallings, page 326, step 3; final paragraph).

14. As per claim 3, Stallings covers a method as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, a match indicates that the received user name and computer identifier are valid (see Stallings, page 326, step 3; constitution of 'Ticket'; final paragraph).

15. As per claim 4, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the method further comprises, before parsing, decrypting the authentication key (see Stallings, page 326, final paragraph).

16. As per claim 7, Stallings covers a method as outlined above in the claim 6 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose that a plurality of users share a server user identifier and corresponding password. However, the use of a shared user identity to logon to a service is notoriously well known in the art. Shared user identities include a range of roles, which cover everything from a default user or guest user for restricted access, to an administrator or root user for privileged access. These types of shared roles are found in popular OS server systems ranging from UNIX to Windows NT. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for a plurality of users to share a server user identifier and corresponding password.

Motivation to combine enables a simple means to classify user access as known to one of ordinary skill in the art.

17. As per claim 10, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). In addition, the method further comprises encrypting the authentication key (see Stallings, page 326, third paragraph).

18. As per claim 11, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). In addition, the method further comprises forwarding the authentication key to a user (see Stallings, page 326, third paragraph).

19. As per claims 13-19 and 21-23, they are apparatus claims corresponding to claims 1-7 and 9-11, and they do not teach or define above the information claimed in claims 1-7 and 9-11. Therefore, claims 13-19 and 21-23 are rejected under Stallings in view of Bryant for the same reasons set forth in the rejections of claims 1-7 and 9-11.

20. As per claims 25-31 and 33-35, they are article of manufacture claims corresponding to claims 1-7 and 9-11, and they do not teach or define above the information claimed in claims 1-7 and 9-11. Therefore, claims 25-31 and 33-35 are rejected under Stallings in view of Bryant for the same reasons set forth in the rejections of claims 1-7 and 9-11.

21. As per claim 42, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). As mentioned above, the computer identifier is identified as a workstation address, but does not specify in greater detail that the workstation address is an IP address. However, TCP/IP is the de facto standard protocol to route messages between network devices. As such, an IP address is an obvious workstation address. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the computer identifier to be identified as an IP address since it enables unique identification of computers networked by TCP/IP as known to one of ordinary skill in the art.

22. As per claim 43, it is a method claim corresponding to claims 1-7 and 9-11 and it does not teach or define above the information claimed in claims 1-7 and 9-11. Therefore, claim 43 is rejected under Stallings in view of Bryant for the same reasons set forth in the rejections of claims 1-7 and 9-11.

23. Claims 12, 24 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bryant, and further in view of Fuh et al. U.S. Patent No. 6,463,474 (hereinafter Fuh).

24. As per claim 12, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose intercepting the

transmitted authentication key from the client to the server by the computer. Fuh teaches an authentication proxy to intercept authentication information, which is implemented as gate-keepers to a secured network and/or service: incoming requests to the secure network and/or service are submitted to the secure network and/or service but authorization is processed by the proxy device unbeknownst to the requesting client. See Fuh, col. 7:62-col. 8:8. It would be obvious to one of ordinary skill in the art at the time the invention was made for the computer to be an authentication proxy that intercepts a client's request to access a server. Motivation to combine enables the secure system to hide organization of the features from those outside the secured system. See Fuh, col. 2:29-32. The aforementioned covers the limitation of claim 12.

25. As per claims 24 and 36 they are claims corresponding to claims 1-7, 12, 13 and 25, and they do not teach or define above the information claimed in claims 1-7, 12, 13 and 25. Therefore, claims 24 and 36 are rejected under Stallings in view of Bryant and Fuh for the same reasons set forth in the rejections of claims 1-7, 12, 13 and 25.

26. Claims 37, 38, 39 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bryant, and further in view of VeriSign "Certification Practice Statement" (hereinafter VeriSign).

27. As per claim 37, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose emailing the

authentication key to the user. VeriSign teaches emailing certified keys to clients. See VeriSign, Section 4.2, 'Method of Communicating Application' for class 1-4. It would be obvious to one of ordinary skill in the art for the generated authentication key to be emailed to the user since email provides a private means to securely communicate information as known to one of ordinary skill in the art and as taught by VeriSign. Ibid. Further, since the server user identifier is incorporated in the authentication key (see claim 1), any change to the server user identifier renders the authentication key obsolete, which necessitates the submission of an updated authentication key based on the updated server user identifier. The aforementioned covers the limitations of claim 37.

28. As per claims 38, 39 and 40, they are method claims corresponding to claims 1-7, 9-11, 36 and 37, and they do not teach or define above the information claimed in claims 1-7, 9-11, 36 and 37. Therefore, claims 38, 39 and 40 are rejected under Stallings in view of Bryant, Fuh, and VeriSign for the same reasons set forth in the rejections of claims 1-7, 9-11, 36 and 37.

29. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bryant, and further in view of Schneier Applied Cryptography (hereinafter Schneier).

30. As per claim 41, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose that the authentication key comprises the computer identifier split into portions and the portions being interposed between the user name, the server user identifier and the server password prior to encryption. However, this feature is a typical result after a permutation step of the recited parts in a method to prepare data as taught by Schneier. See Schneier, page 271, 'The Initial Permutation' of a DES scheme. It would be obvious to one of ordinary skill in the art at the time the invention was made to permute the contents of the authentication key prior to encryption to augment the encryption process. See Schneier, page 271, 2nd paragraph, second sentence. The aforementioned covers claim 41.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
January 18, 2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100